UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/802,255	03/16/2004	Sameh A. Sabet	TCM143	4324

32047 7590 10/02/2006

GROSSMAN, TUCKER, PERREAULT & PFLEGER, PLLC
55 SOUTH COMMERICAL STREET
MANCHESTER, NH 03101

EXAMINER	
TRUONG, LOAN	
ART UNIT	**PAPER NUMBER**
2114	

DATE MAILED: 10/02/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/802,255	SAMEH A. SABET	
	Examiner	Art Unit	
	LOAN TRUONG	2114	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *3/16/2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-26* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *16 March 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This office letter is in response to the application filed March 16, 2004 with claim priority from provision application 60/455136 with priority date of March 17, 2003.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

2. Claims 24-26 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

In regards to claims 24-26, the claims are directed computer-readable medium, such as semiconductor, magnetic, optical or other memory devices, and may be transmitted using any communications technology, such as optical, infrared, microwave, or other transmission technologies (*See specification paragraph 0038*). Therefore, the specified claims do not fall within the technological arts and therefore, is non-statutory. See MPEP § 2106. Examiner suggest applicant to amend the limitation "computer-readable medium" by further adding the limitations of "storing an executable set of software instruction that are executable by a computer system".

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –

(a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

3. Claims 1-2, 6-7, 9, 14, 23 and 24 are rejected under 35 U.S.C. 102(a) as being anticipated by Kakadia (US 6,532,554).

In regard to claim 1, Kakadia disclosed a method for diagnosing faults in a communication network using distributed alarm correlation, said method comprising:

correlating alarm data at a first network node to produce local correlation results (*event correlator, fig. 3, 330)*; and

replicating diagnostic knowledge to a second network node, said diagnostic knowledge being obtained in response to said, local correlation results (*alarm from the alarm monitors are filtered by a local alarm filter in the node. Alarms reported to the network management center are filtered again by an intelligent event correlation, col. 3 lines 20-30).*

In regard to claim 2, Kakadia disclosed the method of claim 1 wherein said correlating alarm data comprises using a generic correlation algorithm to find a root cause of a fault in said network (*rules-based correlation engine, col. 5 lines 39-42).*

In regard to claim 6, Kakadia disclosed the method of claim 1 wherein said alarm data comprises alarm data generated by network elements in said communication network (*art of record targets data communication and communication networks by automatically correlate alarm message to make root cause more apparent to the operator, col. 2 lines 66-67 and col. 3 lines 1-7).*

In regard to claim 7, Kakadia disclosed the method of claim 1 further comprising reporting said diagnostic knowledge and said local correlation results to a higher-level alarm correlation tool (*Alarms reported to the network management center are filtered again by an intelligent event correlation, col. 3 lines 20-30).*

In regard to claim 9, Kakadia disclosed the method of claim 1 wherein said correlating alarm data comprises correlating said alarm data using a local knowledge base at said first network node, said local knowledge base including alarm definitions and correlation rules (*event comparator and alarm monitor compares signal passed between the TCP IP and Ethernet handles of their corresponding specified models and generate alarm message that are passed to event correlator module within the node, fig. 3, col. 5 lines 1-11).*

In regard to claim 14, Kakadia disclosed a distributed alarm correlation system for diagnosing faults in a communication network, said distributed alarm correlation system comprising:

a plurality of node-level alarm correlation tools located at nodes (*event correlator, fig. 3)* in said communication network (*art of record targets data communication and communication networks by automatically correlate alarm message to make root cause more apparent to the operator, col. 2 lines 66-67 and col. 3 lines 1-7)*, wherein each of said node-level alarm correlation tools provide node-level alarm correlation to produce node-level correlation results (*alarms from the alarm monitors are filtered by a local alarm filter in the node, col. 3 lines 20-*

26) and share diagnostic knowledge with other of said node-level alarm correlation tools at other nodes (*alarms are reported to the network management center, col. 3 lines 20-26)*; and

at least one higher-level management level alarm correlation tool located at a network management center (*intelligent event correlation, col. 3 lines 27-30)* in said communication network (*art of record targets data communication and communication networks by automatically correlate alarm message to make root cause more apparent to the operator, col. 2 lines 66-67 and col. 3 lines 1-7)*, wherein each of said node-level alarm correlation tools shares said diagnostic knowledge and said node-level correlation results with said higher-level management level alarm correlation tool (*alarms from local alarm filter in the node are reported to the network management center, col. 3 lines 20-26)*, and wherein said higher-level management level alarm correlation tool provides higher-level alarm correlation to produce higher-level correlation results (*intelligent event correlation utility filter alarms reported again before presenting to network administration staff, col. 3 lines 26-30).*

In regard to claim 23, Kakadia disclosed a distributed alarm correlation system for diagnosing faults in a communication network, said distributed alarm correlation system comprising:

a plurality of node-level alarm correlators (*event correlator, fig. 3)*, located at nodes in said communication network (*art of record targets data communication and communication networks by automatically correlate alarm message to make root cause more apparent to the operator, col. 2 lines 66-67 and col. 3 lines 1-7)*, wherein each of said node-level alarm correlators provides node-level alarm correlation to produce node-level correlation results

(*alarms are filter by a local alarm filter in the node, such that the node reports what is believes to be the root cause, col. 3 lines 20-26)* and share diagnostic knowledge with other of said node-level alarm correlators (*alarms generated by local alarm filter in the node is reported to the network management center to be filter again by an intelligent event correlation utility, col. 3 lines 20-30)*; and

at least one higher-level management level alarm correlator located at a network management center (*intelligent event correlation utility, col. 3 lines 26-30)* in said communication network (*art of record targets data communication and communication networks by automatically correlate alarm message to make root cause more apparent to the operator, col. 2 lines 66-67 and col. 3 lines 1-7)*, wherein each of said node-level alarm correlators shares said diagnostic knowledge and said node-level correlation results with said higher-level management level alarm correlator (*alarms generated by local alarm filter in the node is reported to the network management center to be filter again by an intelligent event correlation utility, col. 3 lines 20-30)*, and wherein said higher-level management level alarm correlator provides higher-level alarm correlation to produce higher-level correlation results (*intelligent event correlation utility further reduce redundant fault information before presenting to network administration staff, col. 3 lines 26-30).*

In regard to claim 24, Kakadia disclosed a machine-readable medium whose contents cause a computer system to perform a method of fault diagnosis in a communication network said method comprising:

correlating alarm data at a first network node to produce local correlation results (*event correlator, fig. 3, 330)*; and

replicating diagnostic knowledge to a second network node, said diagnostic knowledge being obtained in response to said local correlation results (*alarm from the alarm monitors are filtered by a local alarm filter in the node. Alarms reported to the network management center are filtered again by an intelligent event correlation, col. 3 lines 20-30).*

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

4. Claims 3-5, 8, 10-13, 15-22, 25 and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kakadia (US 6,532,554) in further view of Valadarsky et al. (US 7,043,661).

In regard to claim 3, Kakadia does not explicitly teach the method of claim 1 wherein said correlating alarm data comprises using user-defined correlation rules to find a root cause of a fault in said network.

Valadarsky et al. teach the topology-based reasoning apparatus for root-cause analysis of network faults by implementing a rule user interface where the user can added, removed, modified, enabled, disabled or active a rule (*col. 8 lines 53-67).*

It would have been obvious to modify the method of Kakadia by adding Valadarsky et al. topology-based reasoning apparatus for root-cause analysis of network faults. A person of ordinary skill in the art at the time of applicant's invention would have been motivated to make the modification because it would improved fault management system by root cause analysis mechanism of correlator+TRS (*col. 1 lines 35-48).*

In regard to claim 4, Kakadia does not explicitly teach the method of claim 1 wherein said diagnostic knowledge comprises a new correlation rule.

Valadarsky et al. teach the topology-based reasoning apparatus for root-cause analysis of network faults by implementing a rule user interface where the user can added, removed, modified, enabled, disabled or active a rule (*col. 8 lines 53-67).*

Refer to claim 3 for motivational statement.

In regard to claim 5, Kakadia does not explicitly teach the method of claim 1 wherein said diagnostic knowledge comprises at least one of a root cause, an alarm definition, and a corrective action.

Valadarsky et al. teach the topology-based reasoning apparatus for root-cause analysis of network faults by implementing an alarm history to store history information of alarm (*fig. 1, col. 7 lines 49)* and also TRS is operative to anticipate at least one expected alarm associated with at least one respective fault type (*col. 3 lines 52-59).*

Refer to claim 3 for motivational statement.

In regard to claim 8, Kakadia does not explicitly teach the method of claim 1 wherein said correlating alarm data comprises correlating said alarm data using topology configuration information stored locally at said first network node.

Valadarsky et al. teach the topology-based reasoning apparatus for root-cause analysis of network faults by implementing backward traverse for alarms by getting all root causes with distance < max from the current alarm (*fig. 4)*

Refer to claim 3 for motivational statement.

In regard to claim 10, Kakadia teach a method for diagnosing faults in a communication network using distributed alarm correlation, said method comprising:

receiving alarm data locally at network nodes in said communication network (*event comparator and alarm monitor, fig. 3)*;

correlating said alarm data (*rules-based correlation engine, col. 5 lines 39-42)* locally at said network nodes (*event correlator, fig. 3, 330)* using an associated node-level alarm correlation tool to produce correlation results at each of said network nodes nodes (*alarm from the alarm monitors are filtered by a local alarm filter in the node, col. 3 lines 20-30)*;

reporting said correlation results produced locally at said network nodes to respective users at respective said network nodes (*fault information is presented to network administration staff, col. 3 lines 26-30)*;

replicating said diagnostic knowledge to other said network nodes (*alarm from the alarm monitors are filtered by a local alarm filter in the node. Alarms reported to the network management center are filtered again by an intelligent event correlation, col. 3 lines 20-30)*; and

reporting said diagnostic knowledge and said correlation results produced locally at said network nodes to a higher-level alarm correlation tool (*Alarms reported to the network management center are filtered again by an intelligent event correlation, col. 3 lines 20-30).*

Kakadia does not explicitly teach a method for diagnosing faults in a communication network using distributed alarm correlation, said method comprising: adding diagnostic knowledge provided by at least one of said users to a local knowledge base at a respective at least one of said network nodes.

Valadarsky et al. teach the topology-based reasoning apparatus for root-cause analysis of network faults by implementing a rule user interface where the user can added, removed, modified, enabled, disabled or active a rule (*col. 8 lines 53-67).*

Refer to claim 3 for motivational statement.

In regard to claim 11, Kakadia disclosed the method of claim 10 further comprising:

reporting said diagnostic knowledge to other said network nodes (*Alarms reported to the network management center are filtered again by an intelligent event correlation, col. 3 lines 20-30)*; and

adding said diagnostic knowledge to a node knowledge base at said other said network nodes (*alarms filtered by a local alarm filter to suspected root cause are reported to the network management center (col. 3 lines 20-26).*

In regard to claim 12, Kakadia disclosed the method of claim 10 further comprising:

receiving said correlation results at said higher-level alarm correlation tool, said correlation results including root causes of faults determined by local alarm correlation at said network nodes (*alarms filtered by a local alarm filter to suspected root cause are reported to the network management center (col. 3 lines 20-26)*;

correlating said root causes determined at said network nodes to find a higher-level root cause at said higher-level alarm correlation tool (*Alarms reported to the network management center are filtered again by an intelligent event correlation, col. 3 lines 20-30)*;

reporting said higher level root cause to a user of said higher-level alarm correlation tool (*Alarms reported to the network management center are filtered again by an intelligent event correlation, col. 3 lines 20-30)*; and

Kakadia does not teach the method further comprising: adding higher-level diagnostic knowledge provided by said user at said higher-level alarm correlation tool to a higher-level knowledge base in said higher-level alarm correlation tool.

Valadarsky et al. teach the topology-based reasoning apparatus for root-cause analysis of network faults by implementing a TRS to change its decision according to new alarms that have arrived after the decision was made. Furthermore, TRS uses graph traverse in order to find the root cause (*col. 2 lines 10-14).*

Refer to claim 3 for motivational statement.

In regard to claim 13, Kakadia does not teach the method of claim 10 further comprising receiving and storing local topology configuration information at respective said network nodes.

Valadarsky et al. teach the topology-based reasoning apparatus for root-cause analysis of network faults by implementing backward traverse for alarms by getting all root causes with distance < max from the current alarm (*fig. 4)*

Refer to claim 3 for motivational statement.

In regard to claim 15, Kakadia does not teach the distributed alarm correlation system of claim 14 wherein each of said node-level-alarm correlation tools comprises alarm definitions defining alarm groups categorizing alarms generated in said communication network.

Valadarsky et al. teach the topology-based reasoning apparatus for root-cause analysis of network faults by implementing a correlation TRS based on the number of alarms in the incoming group of alarms that are explained by that root-cause (*col. 1 lines 56-65).* TRS can also support manufactured dependent anomalies with different rule for different equipment manufacture (*col. 2 lines 6-10).*

Refer to claim 3 for motivational statement.

In regard to claim 16, Kakadia disclosed the distributed alarm correlation system of claim 15 wherein each of said node-level alarm correlation tools comprises correlation rules for determining a root cause in response to alarms received from network elements (*local event correlator is a rule-based correlation engine, fig. 3, 310, 330, col. 5 lines 39-42).*

In regard to claim 17, Kakadia does not teach the distributed alarm correlation system of claim 16 wherein each of said node-level alarm correlation tools comprises local topology configuration information.

Valadarsky et al. teach the topology-based reasoning apparatus for root-cause analysis of network faults by implementing backward traverse for alarms by getting all root causes with distance < max from the current alarm (*fig. 4)*

Refer to claim 3 for motivational statement.

In regard to claim 18, Kakadia disclosed the distributed alarm correlation system of claim 14 wherein each of said node-level alarm correlation tools includes a local knowledge base (*alarms are filter by a local alarm filter and reports what is to believes to be the root cause of a failure to a network, col. 3 lines 20-26).*

In regard to claim 19, Kakadia disclosed the distributed alarm correlation system of claim 14 wherein each said higher-level alarm correlation tool includes a higher-level knowledge base

(intelligent event correlation utility, col. 3 lines 26-30).

In regard to claim 20, Kakadia does not teach the distributed alarm correlation system of claim 14 wherein each of said node-level alarm correlation tools includes an alarm correlator for correlating network element alarm data with locally stored topology configuration information using user-defined correlation rules.

Valadarsky et al. teach the topology-based reasoning apparatus for root-cause analysis of network faults by implementing backward traverse for alarms by getting all root causes with distance < max from the current alarm *(fig. 4)*

Refer to claim 3 for motivational statement.

In regard to claim 21, Kakadia does not teach the distributed alarm correlation system of claim 14 wherein each of said node-level alarm correlation tools includes a knowledge replicator for replicating new diagnostic knowledge added by a user.

Valadarsky et al. teach the topology-based reasoning apparatus for root-cause analysis of network faults by implementing correlator + TRS based on fault propagation rules and topological network information *(col. 1 lines 35-37)* wherein TRS updates its network topology data on-line and allow the users to change the rules while TRS is still running *(col. 2 lines 20-26).*

Refer to claim 3 for motivational statement.

In regard to claim 22, Kakadia does not teach the distributed alarm correlation system of claim 14 wherein each of said node-level alarm correlation tools allows new diagnostic knowledge to be accepted and added at the discretion of a user.

Valadarsky et al. teach the topology-based reasoning apparatus for root-cause analysis of network faults by implementing a rule user interface where the user can added, removed, modified, enabled, disabled or active a rule (*col. 8 lines 53-67).*

Refer to claim 3 for motivational statement.

In regard to claim 25, Kakadia teach a machine-readable medium whose contents cause a compute system to perform a method of diagnosis in a communication network said method comprising:

receiving alarm data locally at network nodes in said communication network (*event comparator and alarm monitor, fig. 3)*;

correlating said alarm data (*rules-based correlation engine, col. 5 lines 39-42)* locally at said network nodes (*event correlator, fig. 3, 330)* using an associated node-level alarm correlation tool to produce correlation results at each of said network nodes nodes (*alarm from the alarm monitors are filtered by a local alarm filter in the node, col. 3 lines 20-30)*;

reporting said correlation results produced locally at said network nodes to respective users at respective said network nodes (*fault information is presented to network administration staff, col. 3 lines 26-30)*;

replicating said diagnostic knowledge to other said network nodes (*alarm from the alarm monitors are filtered by a local alarm filter in the node. Alarms reported to the network management center are filtered again by an intelligent event correlation, col. 3 lines 20-30)*; and

reporting said diagnostic knowledge and said correlation results produced locally at said network nodes to a higher-level alarm correlation tool (*Alarms reported to the network management center are filtered again by an intelligent event correlation, col. 3 lines 20-30).*

Kakadia does not explicitly teach a method for diagnosing faults in a communication network using distributed alarm correlation, said method comprising: adding diagnostic knowledge provided by at least one of said users to a local knowledge base at a respective at least one of said network nodes.

Valadarsky et al. teach the topology-based reasoning apparatus for root-cause analysis of network faults by implementing a rule user interface where the user can added, removed, modified, enabled, disabled or active a rule (*col. 8 lines 53-67).*

Refer to claim 3 for motivational statement.

In regard to claim 26, Kakadia teach the machine-readable medium of claim 24 wherein said method further comprises:

receiving said diagnostic knowledge from said other network nodes (*alarms filtered by a local alarm filter to suspected root cause are reported to the network management center (col. 3 lines 20-26)*;

reporting said diagnostic knowledge received from said other network nodes to said user at said network node (*alarms reported are presented to network administration staff, col. 3 lines 26-30)*; and or

Kakadia does not teach the method further comprising: adding said diagnostic knowledge received from said other network nodes to said knowledge base in response to said user.

Valadarsky et al. teach the topology-based reasoning apparatus for root-cause analysis of network faults by implementing rule user interface where the user can added, removed, modified, enabled, disabled or active a rule (*col. 8 lines 53-67).*

Refer to claim 3 for motivational statement.

Conclusion

5. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO 892.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Loan Truong whose telephone number is (571) 272-2572. The examiner can normally be reached on M-F from 8am-4pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Scott Baderman can be reached on (571) 272-3644. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Loan Truong
Patent Examiner
AU 2114

SCOTT BADERMAN
SUPERVISORY PATENT EXAMINER